REMARKS

Claims 1 - 14 are pending in the present application. By this Amendment, claim 1 has been amended and new claims 15-24 have been added. No new matter has been added. It is respectfully submitted that this Amendment is fully responsive to the Office Action dated March 23, 2005.

As to the Merits:

As to the merits of this case, the Examiner maintains the following rejections:

1) claim 1 stands rejected under 35 USC 103 (a) as being unpatentable over Werner et al. (Eavesdropping using quantum-nondemolition measurements);

2) claims 2, 5, 8-11, 13 and 14 stand rejected under 35 USC 103(a) as being unpatentable over Werner et al. in view of Bethune (U.S. Patent No. 6,188,768);

3) claims 3, 4, 6 and 7 stand rejected under 35 USC 103(a) as being unpatentable over Bethune; and

4) claim 12 stands rejected under 35 USC 103(a) as being unpatentable over Werner et al. in view of Bartelt et al. (The Wigner Distribution Function –An Alternative Signal Representation in Optics).

Each of these rejections is respectfully traversed.

Regarding Claim 1:

Werner describes the QND eavesdropping that if eavesdropper raises the detection sensitivity to measure more clearly the signal which is a signal of existence and non-existence of the photon, then the correlation probability between the signal detected by the eavesdropper and the signal detected by the recipient, namely the joint-detection probability, becomes lower. This description never discloses "a quantum-mechanical probability distribution change of the difference signal measured by a recipient, which is produced by an eavesdropping operation", namely a quantum-mechanical probability distribution change of quadrature amplitude by an eavesdropping, because the joint-detection probability calculation can not derive a distribution change of quadrature amplitude by an eavesdropping. The probability distribution change of quadrature amplitude by an eavesdropping has firstly derived by the inventor (refer to the Fig. 2 on page 3 of the reference previously submitted, PHYSICAL REVIEW A67, 022308 (2003)).

The DIFFERENCE CURRENT indicated on the Fig. 1 of Werner is derived from the probe light (not from the signal light), and it is an out put of balanced homodyne detector measured by the eavesdropper (not by the recipient) for detecting the phase change created by the existence of the signal photon on the system. The apparatus of the invention also uses a balanced homodyne detector, but it is used by the recipient for detecting the phase signal sent by sender, not by the eavesdropper for detecting the existence or non existence of the photon on the system. Accordingly Werner's apparatus quite differs from the apparatus of the present invention.

The examiner argues that on page 639 and 640, column 1 of Werner, the limitation of "a quantum cipher communication system characterized by the step of detecting eavesdropping based on a change in a quantum-mechanical probability distributions of two amplitude components which are 90 degrees-phase apart from each other measured by a recipient using a difference signal derived from a signal light which change is produced by an eavesdropping operation".

However, in those paragraphs, Werner describes the calculation steps and the thought measurement system for calculating the joint-detection probability, and those descriptions never disclose the above limitation of the invention, because as above mentioned, the joint-detection probability calculation can not derive "a quantum-mechanical probability distribution change of the difference signal measured by a recipient, which is produced by an eavesdropping operation", namely a quantum-mechanical probability distribution change of quadrature amplitude by an eavesdropping, because the joint-detection probability calculation can not derive a distribution change of quadrature amplitude by an eavesdropping. The probability distribution change of quadrature amplitude by an eavesdropping has firstly derived by the inventor (refer to the Fig. 2 on page 3 of the reference previously submitted, PHYSICAL REVIEW A67, 022308 (2003)).

The examiner argues that the joint detection probabilities for both polarizer one and two depend on phase and amplitude of the signal.

But, Werner never describes that the joint-detection probability depends on the phase and the amplitude of the signal sent by the sender, but describes that if an eavesdropper increases

the amplitude of the probe light for detecting more clearly, then the correlation probability between the signal detected by the eavesdropper and the signal detected by the recipient, namely the joint-detection probability, becomes lower.

The examiner argues that the eavesdropping operation is represented by the quantum nondemoliton measure of photon number.

But, the apparatus of the invention uses a phase difference between signal light and reference light as the signal in stead of photon counting, therefore the eavesdropping operation can not be represented only by the quantum nondemoliton measure of photon number, but there are some other method for example "simultaneous measurement attack" and " intermediate basis attack" (refer pages 3 -5 of the reference previously submitted, PHYSICAL REVIEW A67, 022308 (2003)).

The examiner argues that the recombined beams on page 640, column 1 represent the difference signal.

It is assumed that "recombined beams" stated by the examiner is "DIFFERENCE CURRENT indicated on the Fig. 1 of Werner. Then, as above mentioned, the DIFFERENCE CURRENT indicated on the Fig. 1 of Werner is derived from the probe light (not from the signal light), and it is an out put of balanced homodyne detector measured by the eavesdropper (not by the recipient) for detecting the phase change created by the existence of the signal photon on the system. The apparatus of the invention also uses a balanced homodyne detector, but it is used by

the recipient for detecting the phase signal sent by the sender, not by the eavesdropper for detecting the existence or non existence of the photon on the system. Accordingly Werner's apparatus quite differs from the apparatus of the present invention.

The examiner argues that it would have been obvious to one of ordinary skill in the art at the time of the invention to assume the recombined beams to be the difference signal because the recombined beams are derived from an orthogonally polarized light beam that is split in two.

Balanced homodyne detection method is well known method for detecting a phase difference between orthogonally polarized light beams which are made by splitting one beam into two beams. Werner uses it for detecting a photon, but the apparatus of the invention uses it for one of the elements constituting the quantum cipher communication system which does not use photon counting method. Accordingly Werner's apparatus quite differs from the apparatus of the present invention concerning the object and the constitution.

Therefore, it is not possible to assume the recombined beams to be the difference signal.

Regarding Claim 2:

Bethune describes that the signal pulse intensity sent from sender becomes as small as possible to detect its quantum state when it returns to sender. However, in the apparatus of the invention, the intensity of signal light is attenuated at the sender's apparatus and is not returned to the sender from the recipient. Accordingly Bethune's apparatus quite differs from the apparatus of the present invention. Therefore it is not obvious to one of ordinary skilled person in

the art to reach the constitution of the invention from Bethune.

Bethune describes on column 2 lines 51-57, that "the key information is decoded at the sender that uses two detectors, one of which detects a polarization state corresponding to the phase difference between the two phase shifts---". From these description, it is apparent that in Bethune, the signal recombined creates a polarization depending on the phase difference added by the sender and recipient, then the polarization leads the signal recombined to either of the detector D0 or D1 depending on the direction of the polarization, and the phase added by the sender and the receipt is determined by which the detector detected the photon of the signal recombined. On the other hand, in the apparatus of the invention, the signal light and the reference light are superimposed at the recipient side, then the difference signal of the balanced homodyne detector, which depends on the phase difference added by the sender and recipient, is measured, and the phase added by the sender and the receipt is determined by comparing the difference signal with a threshold value. Accordingly Bethune's apparatus quite differs from the apparatus of the present invention concerning the method of getting a privacy key and the constitution.

Therefore it is not possible to obtain the apparatus of the invention by combining the teaching of Bethune within the system of Werner.

Additionally, in the current claim amendment, the applicant uses the term of "optical balanced homodyne detector" which is not described in the firstly submitted specification. But it is obvious to one of ordinary skill in the art that the term is uniquely and directly derived from

the detectors indicated in the Fig. 1 and Fig. 6 attached with the firstly submitted specification and the descriptions concerning the figures of the firstly submitted specification.

New Claims 16-24

New independent claim 16 is based on the Fig. 1 attached to the specification firstly submitted and its description concerning to the Fig. 1. New independent claim 17 is based on the Fig. 6 attached to the specification firstly submitted and its description concerning to the Fig. 6. New independent claim 15 is the generic claim of the new claims 16 and 17.

A quantum cipher communication system is a system that uses signal light at single-photon level because of detecting eavesdropping. As described in Background Art of the specification, quantum cipher communication system so far proposed is called a photon counting system that detects an existence of the photon by a single -photon detector and assigns signal bit 1 and bit 0 corresponding to the existence and the non existence detected by the single-photon detector.

However, there is no single-photon detector that has enough quantum efficiency to detect single photon at telecommunication wavelength (between 1.3 micro-meter and 1.6micro-meter) in practice. Therefore the quantum cipher communication system so far proposed in practical suffers from a reduced transfer rate caused by a loss in detection. Moreover in principle the loss does not give a distinction from an attempt to eavesdrop, therefore, there is a problem that the detection of eavesdropping is difficult.

The apparatus of the invention is provided for solving the above problems, and it uses a phase difference between a signal light and a reference light which are 90degrees-phase apart each other as the signal in stead of photon counting or photon counting using polarization states of a single photon, wherein the signal light comprises single photon or so in number and the reference light comprises several millions photons. The phase difference is produced by a sender and a recipient adding a phase on the signal light or the reference light. The apparatus has an optical balanced homodyne detector which detects the phase difference as a difference signal of the detector, and the phase difference is determined from the difference signal by comparing with a threshold value. Since homodyne detection makes it possible to detect very weak signal light by increasing reference light intensity, it is possible to detect the phase difference with a performance very close to a theoretical detection limit, even if the signal light is at single-photon level, and even if the detector is common-use photo diodes.

The system described in the reference cited by the examiner Bethune is a photon counting system, because, as described on column 6 lines 23-24, its return pulses are recombined into a single return signal, then, as described on column 6 lines 64-66, the single return signal is directed to detector D0 depending on its polarization, or, as described on column 7 lines 8-9, the single return signal is directed to detector D1 depending on its polarization, and, as described on the table shown in the lower part of column 7, the signals detected by D0 and D1 are only the existence or non existence of the single return signal. Therefore this system can not overcome the above problem that there is no photon detector that has enough quantum efficiency to detect

single photon in practice, therefore with this system the transfer rate is low and the detection of eavesdropping is difficult.

In view of the aforementioned amendments and accompanying remarks, Applicant submits that that the claims, as herein amended, are in condition for allowance. Applicant requests such action at an early date. If the Examiner believes that this application is not now in condition for allowance, the Examiner is requested to contact Applicant's undersigned attorney to arrange for an interview to expedite the disposition of this case.

If this paper is not timely filed, Applicant respectfully petitions for an appropriate extension of time. The fees for such an extension or any other fees that may be due with respect to this paper may be charged to Deposit Account No. 50-2866.

Respectfully submitted,

WESTERMAN, HATTORI, DANIELS & ADRIAN, LLP

Thomas E. Brown
Attorney for Applicant
Registration No. 44,450

TEB/jl

1250 Connecticut Avenue, NW
Suite 700
Washington, D.C. 20036
(202) 822-1100